K2 SOFTWARE, INC.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT
FOR THE K2 CLOUD SERVICE

FOR THE PERIOD OF MARCH 1, 2019, TO FEBRUARY 29, 2020

Attestation and Compliance Services

INDEPENDENT SERVICE AUDITOR'S REPORT

To K2 Software, Inc.:

Scope

We have examined K2 Software, Inc.'s ("K2") accompanying assertion titled "Assertion of K2 Software, Inc. Service Organization Management" ("assertion") that the controls within K2's K2 Cloud Service ("system") were effective throughout the period March 1, 2019, to February 29, 2020, to provide reasonable assurance that K2's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

K2 uses a subservice organization for cloud hosting services. The description of the boundaries of the system indicates that complimentary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at K2, to achieve K2's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such

Service Organization's Responsibilities

K2 is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that K2's service commitments and system requirements were achieved. K2 has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, K2 is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and systems requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that controls were not effective to achieve K2's service commitments and system requirements based on the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve K2's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that K2's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within K2's K2 Cloud Service were effective throughout the period March 1, 2019, through February 29, 2020, to provide reasonable assurance that K2's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects

Schellman & Company, LLC

Tampa, Florida
April 21, 2020

ASSERTION OF K2 SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within K2 Software, Inc.'s ("K2") K2 Cloud Service ("system") throughout the period March 1, 2019, to February 29, 2020, to provide reasonable assurance that K2's service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the system is presented below and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period March 1, 2019, to February 29, 2020, to provide reasonable assurance that K2's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. K2's objectives for the system in applying the applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period March 1, 2019, to February 29, 2020, to provide reasonable assurance that K2's service commitments and systems requirements were achieved based on the applicable trust services criteria.

SYSTEM DESCRIPTION OF THE K2 CLOUD SERVICE

Company Background

Founded in 1998, in Johannesburg, South Africa, two young software developers had a vision to make process automation easy and change how business was done. Since then, K2 has grown into a business application software company with five offices and over 500 employees across the globe. K2's business applications and tools help companies create successful solutions and increase agility. More than 1.5 million users in over 84 countries, including 30 percent of the Fortune 100, are using K2 to save money, reduce risk and grow revenue.

Description of Services Provided

Core Services

Through the use of the K2 Cloud Service, organizations can build and deploy low-code business applications that are agile, scalable, and reusable, resulting in modern processes that easily connect people, data, decisions, and systems. K2 supports organizations who need to manage business growth for both today and the future by giving them the tools they need to build business process applications and run them from anywhere, on any device.

K2 Cloud is a cloud-based, Software-as-a-Service (SaaS) offering that provides K2 software and supporting components as a service, in which software and associated maintenance operations can be licensed as a comprehensive service managed by K2. Within K2 Cloud, customers are provided:

- Fully web-based tooling experience – three different persona-based experiences that focus tooling on the specific needs of the customer.
- Support for authentication and authorization – by integrating into Microsoft Azure Active Directory, customers can utilize their investment in both on-premises and cloud-based identity management.
- Line-of-business integration – K2 Cloud allows customers to integrate into other mission critical applications where business data typically resides, but surface and update that data from applications designed on K2; seamlessly combining multiple data sources into a single composite application.
- Mobile app platform – applications built on K2 Cloud can be surfaced onto leading mobile device platforms so that users can interact with forms and workflows on any screen or experience.
- Enterprise workflow platform – providing the abilities to both model and execute enterprise workflow processes that can span groups, users, and systems within an organization.

With the K2 Cloud Service, K2 provides and maintains the platform that enables customers to build applications on K2, without the overhead of setting up, hosting, and maintaining K2 environments. The customer does not manage or control the underlying infrastructure (such as network, servers, operating systems, storage, or K2 software components), but retains control over the application development cycle and deployed applications.

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Principle Service Commitments and System Requirements

K2 designs its processes and procedures related to the K2 Cloud Service to meet its objectives for its K2 Cloud Service. Those objectives are based on the service commitments that K2 makes to user entities, the laws and regulations that govern the provision of the K2 Cloud Service, and the financial, operational, and compliance requirements that K2 has established for the services.

Security and availability commitments to user entities are documented and communicated in the customer quotation that references the description of the service offering provided online, as well as the user guide and service policies provided to the customers.

The principal security and availability commitments are standardized and include, but are not limited to, the following:

- K2 shall make services available to the customer 24 hours a day, seven (7) days a week except for interruptions by reason of maintenance or downtime beyond K2's reasonable control.
- K2 is committed to the runtime and uptime of K2 Cloud Service at no less than 99.9%. However, due to the nature of end user internet connectivity and network access to the K2 Cloud Service being completely outside the control of the K2 Cloud platform, this availability guarantee is exclusively applied to the uptime of the K2 Cloud platform runtime and services and does therefore not guarantee the customer internet access or network connectivity to the K2 Cloud Service.
- K2 is committed to maintaining the appropriate organizational and technical controls to protect customer data entrusted to K2.
- K2 shall communicate any maintenance changes and software upgrades to customers as per the defined service level agreement.
- K2 is committed to undergo a security audit and perform a penetration test of the K2 Cloud Service on an annual basis.
- K2 is committed to adhere to the ISO/IEC 27001:2013 standard and maintain the certification.

K2 establishes operational requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other system requirements. These requirements include the monitoring of production systems for performance and system anomalies by the information technology (IT) operations personnel and the third-party service provider, the database backup and recovery processes, the account and password management processes, the vulnerability assessment and remediation processes, the employee background check and security awareness training, and the necessary system change management procedures to support the requisite authorization, documentation, testing, and approval of system changes.

K2's information security policies define an organization-wide approach to how systems and data are protected, how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired, trained, and managed.

In accordance with K2's assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to each system users, in each individual case.

Infrastructure and Software

K2 has outsourced infrastructure resource requirements to Microsoft Azure. Microsoft Azure is a cloud computing platform and infrastructure created by Microsoft for building, deploying, and managing applications and services through a global network of Microsoft-managed data centers. Microsoft Azure provides SaaS, Platform as a service (PaaS) and Infrastructure as a Service (IaaS) services, and supports many different programming languages, tools, and frameworks, including both Microsoft-specific and third-party software and systems. The K2 Cloud Service is built on the Microsoft Azure platform and uses many features of Microsoft Azure. New customer instances are created for each customer on the K2 platform.

K2 does not own or maintain any of the hardware located in the Microsoft data centers and operates under a shared security responsibility model, where Microsoft is responsible for the security of the underlying cloud infrastructure (i.e. physical infrastructure, geographical regions, availability zones, edge locations, operating, managing and controlling the components from the host operating system, virtualization layer and storage). K2 is responsible for securing the K2 platform deployed in Microsoft Azure (i.e. customer data, applications, identity access management, operating system, and network firewall configurations).

Production servers and client facing applications are logically and physically separated from K2's internal corporate information systems. The IT team maintains all internal systems. The Cloud Operations team maintains the production systems in the Microsoft Azure environment.

The in-scope infrastructure consists of multiple applications, operating system platforms and databases, as shown in the table below:

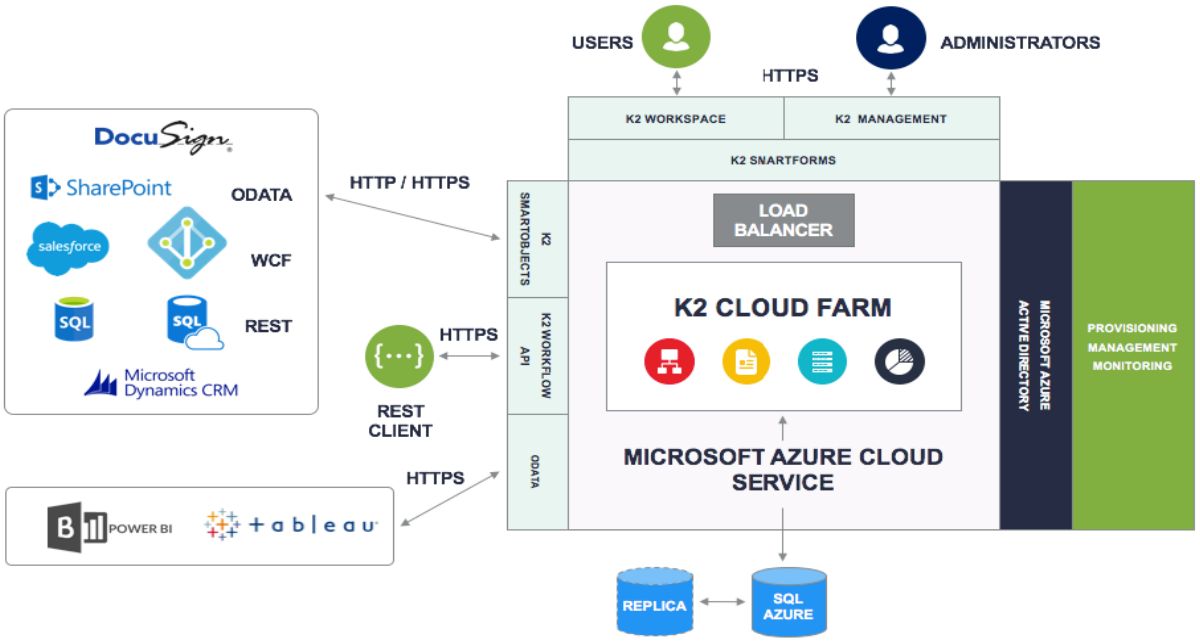
Primary Infrastructure			
Production Application	**Business Function Description**	**Operating Systems**	**Physical Locations**
K2 Cloud	Front-end application which provides the platform for the K2 Cloud Service.	Windows Operating Systems (OS)	Microsoft Azure - Tukwila, Washington
Microsoft Azure Service	Virtualized network and processing infrastructure to host the K2 Cloud Service.	N/A	
Landlord - A collection of servers, configuration databases, workflows, scripts, and user interfaces.	Landlord orchestrates the K2 Cloud environments' creation, updates, and deletion. Cloud Operations team uses Landlord to maintain an environment throughout its lifetime. Landlord provides automation and user interface for the Cloud Operations engineers to take various actions.	Windows OS	
BlackOps - A collection of worker roles, sync / job / configuration databases and user interfaces.	BlackOps fulfills Landlord's requests by making the Application Program Interface (API) calls to third-party providers like Microsoft Azure Domain Name System (DNS), Pingdom, etc.	Windows OS	
Operations Management Suite	Cloud-based agent-driven analysis and logging service.	N/A	
Windows Active Directory (AD) and Azure Active Directory (AAD)	AD domain utilized to control access to the corporate and production networks.	Windows OS	
SQL Azure	Database software to support both applications and store client data.	Windows OS	

Also, the following third-party applications are utilized to support the production systems:

- Pingdom - Is a service that tracks the uptime, downtime, and performance of the K2 Cloud customer environments and internal IT systems. Pingdom monitors websites from multiple locations so that it can distinguish genuine downtime from routing and access problems and alerts IT personnel as required.
- Amazon Route 53 DNS - Highly available and scalable cloud DNS web service. Designed to route end users to K2 Cloud by translating names like kuid.onk2.com into the numeric IP addresses that computers use to connect to each other. Amazon Route 53 DNS effectively connects user requests to infrastructure running in Microsoft Azure.
- Thycotic Secret Server - An online password manager. Has multiple layers of built-in security with easy access management for K2 Cloud operations, robust segregation of role-based duties, Advanced Encryption Standard (AES) 256-bit encryption, and out of the box reports to demonstrate compliance.

- Ticket Management System (TMS) - Internal ticketing system used by IT and operations personnel for recording security incidents, access requests and any configuration change management tasks.

High-level Architecture Diagram:



People

- Executive management –responsible for supporting and promoting the security program within the company, overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- Security committee – responsible for providing support for the business by assuring the confidentiality, integrity, and availability of company information assets. The Security Committee discusses security topics, reviews key security metrics, and approves security policies.
- Information security management systems (ISMS) manager – responsible for implementing and maintaining the ISMS. Also, manages security incident recording and risk management.
- Security administrators – responsible for the management of security controls and configurations within the information systems they support. They implement security mechanisms and maintain the requisite technical expertise to support them. They ensure systems and services comply with all approved corporate information security policies, standards, and procedures.
- Managers – responsible for ensuring that employees and contractors, under their responsibility, adhere to applicable policies and procedures.
- Internal IT team – responsible for building and maintaining network and infrastructure for the k2.com website and local service domains. Including AD, Exchange, fileservers, K2 application infrastructure, websites and webserver, advanced threat monitoring (ATA), System Center Operations, and Internal K2 infrastructure.
- Cloud Operations team – responsible for developing, maintaining, and supporting customer environments that are located within Microsoft Azure. The cloud team deploys and configures a cloud-based SaaS offering that is built using K2 software.

Procedures

Access, Authentication and Authorization

Documented information security policies and procedures are in place to govern information security standards. Access to system information, including confidential information, is protected by authentication and authorization mechanisms. The IT teams are responsible for assigning and maintaining access rights to the production environment. In order to gain access to the production environment a user must authenticate first via an AAD services and requires a user account and password. Authentication rules are enforced through AAD including unique user account and password minimum length. In addition, administrative access privileges within the production environment are restricted to authorized personnel. Documented standard build procedures are utilized for installation and maintenance of production servers. The systems utilize transport layer security (TLS) encryption for communication sessions. Production resources are protected by firewalls and Microsoft Azure security rulesets designed to filter unauthorized Internet traffic and to deny any activity not previously defined, the firewall configurations are reviewed by IT management on a quarterly basis. Production systems are hosted on Microsoft Azure and access to the Microsoft Azure platform is restricted to authorized personnel. In-scope systems in Microsoft Azure are configured to log access related events.

Access Requests and Access Revocation

Management has established controls to ensure that access to confidential data is restricted to those who require access. A formal process has been established for managing user accounts and controlling access to the production environment. Prior to granting an individual access upon employment, the access request must be reviewed and approved by the employee's manager. Upon notification of an employee termination, human resources personnel create a termination checklist which is shared with the IT department to ensure that employees do not retain system access subsequent to their termination date. Management requires access requests and access revocations to be formally documented to ensure activities are completed for the addition, modification, and revocation of system and software access privileges. On a quarterly basis, management performs a user access review to verify users with access to the productions systems are authorized.

Documented policies and procedures are in place to guide personnel in the customer implementation and setup process, to remove data and software stored on equipment, and to render such data and software unreadable upon a customer termination. A ticketing system is utilized to track the status of customer onboarding activities and customer data must be removed or obfuscated after the relationship with the customer has been terminated, or on customer demand.

Change Management

Documented policies and procedures are in place to guide personnel in the in-scope systems change management process, and to ensure any unauthorized changes are not made to production systems. A change management meeting is held on a weekly basis to discuss and communicate the ongoing and upcoming projects that affect the in-scope systems. The change management process adds oversight, visibility, and control of changes to the K2 environment. Team Foundation Server (TFS) change management ticketing system is utilized to log and track in-scope system changes. Application development is performed by the development team in South Africa and the build files are sent to the Cloud Operations team in Seattle, Washington.

Changes made to the in-scope systems are initially authorized and tested when required by the K2 development team. Source code is stored within a version control system and access to the source code is restricted to authorized personnel. Once the developed build files are sent to the Cloud Operations team, additional testing is performed. The Cloud Operations team performs quality assurance (QA) testing in a QA environment which is segregated from the production environment. The production environment is logically and physically segmented from development and test environments. Changes must follow a formal approval process prior to implementation. Further, any security incidents that require a change to the in-scope systems follow the standard change control process.

The ability to implement changes to production is restricted to authorized personnel. Additionally, segregation of duties is established to ensure personnel who have access to source code do not have access to the production environment. Standard back out procedures are documented for each typical implementation to allow for rollback of changes when changes impair system operations. More complex back out procedures will be developed for non-standard implementations.

Emergency Changes

In the event that an emergency application change must be implemented, the change is required to follow the established change control process. The speed at which approvals are obtained is accelerated.

Data Backup and Disaster Recovery

K2 operates under a hosted environment model at Microsoft Azure. K2 does not own or maintain hardware located at Microsoft Azure data centers. Responsibility over the security of the underlying cloud infrastructure (i.e. physical infrastructure, geographical regions, availability zones, edge locations) rests with Microsoft Azure. K2 is responsible for the security of the platform deployed in Azure.

K2 has implemented a set of automated monitoring tools and notification services to help monitor the system's performance and capacity. These tools allow IT personnel to identify and triage any system issues and ensure the availability of service. K2 relies on Microsoft Azure to share the load across data centers and spool up new instances of the platform during system outages or increased capacity demands to ensure continual service.

Microsoft Azure's SQL database business continuity feature allows production databases to be restored to any specific time in the prior 35 days. K2 implemented backup and recovery procedures to guide personnel in performing backup of production systems. Backup of the production data is performed on a daily basis. Backup restorations are performed on the production (cloud hosting) environment on as needed basis.

K2 has implemented a disaster recovery plan, which is updated on an annual basis. The plan is tested on an annual basis, and the executive management implements any required training or adjustments to the plan as a result of the testing. The disaster recovery plan also guides personnel in disaster identification and declaration, business continuity process (BCP) activation and communication and strategies for restoration. Microsoft Azure is responsible for implementing and maintaining physical and environmental security controls around backup and disaster recovery infrastructure and is also responsible for monitoring the equipment and related services contained in the Microsoft Azure data centers.

Incident Response

Any event that exposes company or customer data or an event that puts workers or users at risk is considered a security incident. Documented security incident management policy escalation procedures are in place and available to personnel via the company intranet site for reporting security incidents. For each incident, an incident response lead is assigned to take action. IT personnel utilize a ticketing system and a security incident template to document security violations, responses, and resolution. Any security incidents requiring a change to the system follow the standard change control process.

System Monitoring

K2 monitors the daily business and operational activities, including the internal control environment, as a routine part of business and has implemented a set of network and application tools for monitoring the production environment. Further predefined rules are utilized in Microsoft Azure to monitor the availability and usage of production systems and alert IT personnel when pre-defined thresholds are met. Additionally, the third-party logging and monitoring systems are utilized to monitor uptime of production customer instances on the K2 platform.

Penetration testing, security reviews and vulnerability scans are performed on an annual basis and when needed, remediation plans are created and monitored through resolution. Further, system logs are stored within Microsoft Azure and can be accessible via the log aggregation system.

[Intentionally Blank]

Data

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Customer data	Output data is available to customers via the customer K2 Cloud interface.	Confidential

Subservice Organizations

The cloud hosting services provided by Microsoft Azure were not included within the scope of this examination. The following table presents the applicable Trust Services criteria that are intended to be met by controls at Microsoft Azure, alone or in combination with controls at K2, and the types of controls expected to be implemented at Microsoft Azure to meet those criteria.

Control Activity Expected to be Implemented by Microsoft Azure	Applicable Trust Services Criteria
Microsoft Azure is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the K2 systems reside.	CC6.1, CC6.2, CC6.3, CC6.5, CC6.6, CC6.7, CC7.1, CC7.2
Microsoft Azure is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC6.4, CC6.5, CC7.2
Microsoft Azure is responsible for ensuring capacity demand controls are in place to meet K2's availability commitments and requirements.	A1.1
Microsoft Azure is responsible for ensuring environmental protection controls are in place to meet K2's availability commitments and requirements.	A1.2